Secure NT Installation and Configuration Guide Briefing

15 & 16 January 1998

Mr. Robert P. Blaisdell
Electronic Systems Center DII AF
email: rpb@mitre.org
(781) 271-5757

Background

- **May 97 NTAG**
  - Concerns over Lack of Guidance on Securing NT under the DII COE Identified (Action Item 9705-02 & 03)
- **June 97 NTAG**
  - Security Issues Briefings (Action Items 9706-02, 05, & 06)
- **July 97 NTAG**
  - NT Configuration Guidance Briefed by Jack Wool & Carol Wickham
- **July 97**
  - GCCS-T Security Procedures Written for DII COE

Background

- **August 97**
  - DoDIIS completed a Security Assessment of the DII COE Kernel (including NT) at Rome Laboratory
- **October 97 NTAG Reorganization Message**
  - Security of NT Important Work Area
- **October 97**
  - Draft Secure NT Installation & Configuration Guide Distributed to NTAG Members for Comment
- **13/14 November 1997**
  - Sub Working Group Meeting of NTAG/Security at CENTCOM to Review Document

Background

- **5 December 97 AOG**
  - Document Briefed and Guide Release for 60 Day C/S/A Review
    - Formal Comments Should Be Sent to SSTWG and/or NTAG Chairs
- **12 December 97**
  - Microsoft Federal Security Summit
- **January 98 DII AF**
  - Segmentation of GOTS Security Utilities
  - Design Walkthrough

Scope of the Document

- **Covers the Secure DII COE Configuration of Microsoft’s Windows NT v4.0 Operating System (Workstation and Server)**
  - Hard Guidance For All Security Levels
    - Examples (C2 Utility Evaluation, Protection of Admin Accounts, Backup of Audit Logs, etc.)
  - Local Options to be Determined by Local ISSO
    - Examples (Audit requirements, Account Group Permissions/Names, Implementation of Additional Security Utilities, etc.)

Scope of the Document

- **Work to be Done**
  - Develop Process for Securing the NT Environment after Loading Applications
  - Automating the Procedures for an Enterprise Rollout
  - Evaluating the Impacts of New Security Model used by Microsoft Windows NT v5.0

Document Outline

- Chapter 1 Introduction
- Chapter 2 Pre-Installation
- Chapter 3 Blue Screen Installation
- Chapter 4 Graphical Window Installation
- Chapter 5 C2 Configuration Manager
- Chapter 6 File System Configuration
- Chapter 7 Audit Policy Configuration
- Chapter 8 Registry Configuration
- Chapter 9 User Manager for Domains Configuration

Document Outline

- Chapter 10 User Account Policy Configuration
- Chapter 11 User Environment Profile Configuration
- Chapter 12 System Policy Configuration
- Chapter 13 User Rights Policy Configuration
- Chapter 14 Domain Model Configuration (Trusts)
- Chapter 15 Control Panel Configuration
- Chapter 16 Additional Security Measures

What’s Required?

- **Copy of the Commercial NT Kernel**
- **Copy of the DII COE Installer**
- **Copy of the Secure NT Installation and Configuration Guide**
- **Well Thought Out and Locally Cleared Security Configuration Options**
- **Copy of C2 Utility supplied by the NT Resource Kit**
- **Latest O/S Service Pack (Currently SP3) & Hot Fixes**

  ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3

  ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3

Actions for NTAG

- **Members Review of the Draft Secure NT Configuration & Installation Guide**
- **Consensus Formulation for the Architecture Oversight Group (AOG)**
- **Update of the DII COE Documentation to Reflect Guidance**
  - I&RTS, Kernel Installation Guide, etc.
- **Development of Procedures for Securing NT Environment after Loading Applications**

Actions for NTAG

- **Development of Automating the Procedures for an Enterprise Rollout**
  - Templates & Scripts
  - Commercial Disk Imaging Products
- **Determining the Impact of New Windows NT v5.0 Security Model**

NT Advisory Group
15 & 16 January 1998
Discussion and Comments

Mr. Robert P. Blaisdell
Electronic Systems Center DII AF
email: rpb@mitre.org
(781) 271-5757